IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method to manage secure communications implemented in a computer-readable ~~storage~~ medium and to execute on a proxy, ~~for performing~~ the method, comprising:

establishing a secure session on a secure site with an external client that communicates from an insecure site;

detecting access attempts during the secure session directed to insecure transactions, the insecure transactions identified as links to a site that is external (external site) to, not controlled by, and not recognized by the secure site, and wherein the access attempts are directed to the insecure transactions having references to resources of the external site; and

transparently managing the access attempts by pre-acquiring content from the external site by accessing the links on behalf of the external client to pre-acquire the content and by scanning and inspecting the content within the secure site before determining whether the content should be made available to the external client during the secure session, and wherein at least one access attempt associated with at least one piece of the content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined to have been tampered with ~~part of a pre-defined list of unacceptable references that are not recognized by the secure site~~, and wherein the true insecure reference is entirely removed from the content before the content is supplied to the external client.

2. (Previously Presented) The method of claim 1 wherein the detecting further includes translating any non-secure links into secure links for some of the insecure transactions before presenting results of the access attempts to the external client.

3-5. (Cancelled).

6. (Previously Presented) The method of claim 1 wherein managing includes at least one or

more of:

permitting normally occurring security warnings to present messages to the external client by taking no action;

generating for and displaying to a custom warning message that is presented to the external client;

issuing alerts, notifications, or advisories to a monitoring entity or log; and

determining a number of the links are low-risk to or trusted by the secure site and thereby suppressing normally occurring security warnings from being presented to the external client.

7. (Cancelled).

8. (Currently Amended) A method to manage secure communications implemented in a computer-readable ~~storage~~ medium and to execute on a proxy, ~~for performing~~ the method, comprising:

detecting insecure transactions occurring during a secure session, wherein the insecure transactions result from actions requested by an external client participating in the secure session;

inspecting the insecure transactions in advance of satisfying the actions requested by pre-acquiring content associated with the insecure transactions before making available to the external client, and wherein the insecure transactions are associated with links to an external site located outside a secure site associated with the secure session, and wherein content are pre-acquired from the external site via the links and inspected and scanned on behalf of the external client within the proxy; and

making a determination based on ~~in response to~~ the inspection for taking processing actions including one or more of the following: ~~for~~ permitting some of the insecure transactions to proceed unmodified by performing the actions requested for the external client; [[,]] permitting some of the insecure transactions to proceed in a modified fashion; [[,]] and denying some of the insecure transactions by denying the actions requested, and wherein some of the insecure transactions that are denied are identified as references that have a World-Wide Web

(WWW) cookie associated with their headers ~~to a pre-defined list of unacceptable references that are not recognized by the secure site~~, and wherein these references are entirely removed from the content before the content is supplied to the external client.

9. (Cancelled).

10. (Currently Amended) The method of claim 8, wherein the making a determination further includes, permitting some of the insecure transactions to proceed in the modified fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links to HTTP over Secure Sockets Layer (HTTPS) in order to suppress ~~the~~ security warning messages.

11. (Cancelled).

12. (Previously Presented) The method of claim 8 wherein the making a determination further includes permitting some of the insecure transactions to proceed unmodified by permitting normally occurring security warnings to be presented to the external client before satisfying the external client access attempt to reference the external site.

13. (Previously Presented) The method of claim 8 wherein the making a determination further includes permitting some of the insecure transactions to proceed in a modified fashion by transparently processing the external client access attempt within a proxy making the external client access attempt appear to be part of the secure session.

14. (Currently Amended) The method of claim 8 wherein the making a determination further includes denying the some of the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of a ~~the~~ denial.

15. (Previously Presented) The method of claim 8 wherein the making a determination further includes denying the some of the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access

attempt.

16. (Currently Amended) A secure communications management system implemented in a computer-readable ~~storage~~ medium and to process on a machine, comprising:

a secure communications manager processing on the machine associated with a secure site and which manages a secure session with an external client that is associated with an insecure site; and

a proxy that processes on the machine within the secure site and which interacts with the secure communications manager in order to inspect insecure communications requested by the external client during the secure session by pre-acquiring content associated with the insecure communication before making available the content accessible to the external client, and wherein the proxy selectively processes the insecure communications on behalf of the external client within the secure session, and wherein the content are acquired from an external site not associated with the secure site and the external client and the content are scanned and inspected within the secure site to determine whether to make the content accessible to the external client, and where at least one piece of the content is associated with true insecure references identified as particular references having metadata that are associated with World-Wide Web cookies ~~via a pre-defined list of unacceptable references that are not recognized by the secure site~~, and wherein the true insecure references are entirely removed from the content before the content is supplied to the external client.

17. (Original) The secure communications management system of claim 16 wherein the secure communications manager translates Hypertext Transfer Protocol (HTTP) insecure communications into HTTP over Secure Sockets Layer (HTTPS) secure communications during the secure session.

18. (Previously Presented) The secure communications management system of claim 16 wherein the proxy selectively modifies a number of the insecure communications and permits them to proceed thereby suppressing normally occurring security warning messages that the secure communications manager issues.

19. (Previously Presented) The secure communications management system of claim 16 wherein the proxy selectively leaves a number of the insecure communications unchanged and permits secure communications manager to issue security warning messages to the external client.

20. (Currently Amended) The secure communications management system of claim 16 wherein the proxy selectively denies a number of the insecure communications to proceed and at performs at least one of reports the denial to another entity and records a ~~the~~ denial in a log.

21. (Previously Presented) The secure communications management system of claim 16, wherein the proxy selectively issues custom warning messages or explanations to the external client regarding a number of the insecure communications.

Claims 22-30. (Cancelled).